Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	PS Docket No. 10-146
National Broadband Plan Recommendation	)	
to Create a Cybersecurity Roadmap	)	GN Docket No. 09-51
	)	
_____	)	

COMMENTS OF SPRINT NEXTEL CORPORATION

Charles W. McKee
Vice President, Government Affairs
Federal & State Regulatory

Maria L. Cattafesta
Senior Counsel, Government Affairs

Sprint Nextel Corporation
900 7th Street, N.W., Suite 700
Washington, D.C. 20001
703-433-3786

September 23, 2010

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	PS Docket No. 10-146
National Broadband Plan Recommendation	)	
to Create a Cybersecurity Roadmap	)	GN Docket No. 09-51
	)	
	)	

COMMENTS OF
SPRINT NEXTEL CORPORATION

Sprint Nextel Corporation ("Sprint") submits the following comments in response to the Federal Communication Commission's ("FCC" or "Commission") Public Safety and Homeland Security Bureau ("PSHSB") Public Notice DA 10-1354, issued August 9, 2010, which asks whether the Commission should create a Cybersecurity Roadmap ("Roadmap") to "identify vulnerabilities" and "develop countermeasures and solutions" in response to growing cyber threats. Cybersecurity is a matter of critical interest to all telecommunications carriers. The proposed Roadmap, however, could undermine and unnecessarily duplicate current governmental and carrier activities addressing cybersecurity vulnerabilities and threats. Therefore, Sprint respectfully suggests that the Commission focus its efforts on supporting the Communications Security, Reliability and Interoperability Council's ("CSRIC") cybersecurity best practices work and developing an educational outreach program to protect consumers and small businesses.

I. Introduction and Summary

The Commission's PSHSB seeks public comment on "the creation of a Cybersecurity Roadmap to identify vulnerabilities to communications networks or end-users and to develop

countermeasures and solutions in preparation for, and response to, cyber threats and attacks in coordination with federal partners."[1] The PSHSB's inquiry emanates from the National Broadband Plan recommendation that the FCC develop a Roadmap "to identify the five most critical cybersecurity threats to communications infrastructure and its end users and establish a two-year plan, including milestones, for the FCC to address these threats."[2] As part of its inquiry, the PSHSB also asks what role, if any, the FCC should play in addressing cyber vulnerabilities and how it should coordinate its efforts with other government agencies.[3]

While Sprint shares the PSHSB's valid concerns about the dangers of cyber threats, the proposed Roadmap also raises many potential concerns. A Roadmap would likely reveal highly sensitive cybersecurity information, which hostile actors can then use to create their own roadmap to further their malicious activities. In addition, the proposed Roadmap may become quickly outdated and could inadvertently impede rapid responses to emerging cyber threats. In any event, the Commission may want to suspend consideration of such cybersecurity activities until its role in the emerging federal cybersecurity landscape is defined, and it completes its broader broadband Notice of Inquiry.

In the meantime, Sprint suggests that the Commission continue to support CSRIC's cybersecurity best practices work as a means to help bolster cyber defenses. In addition, the Commission should consider launching or participating in a cybersecurity outreach campaign to

---

[1] *FCC Seeks Public Comment on National Broadband Plan Recommendation to Create a Cybersecurity Roadmap*, Public Notice, DA 10-1354, rel. Aug. 9, 2010 at 1 (*Public Notice*).

[2] *Public Notice* at 1 (*citing* Omnibus Broadband Initiative, Federal Communications Commission, *Connecting America: National Broadband Plan* (March 2010) at 123 (Recommendation § 16.5)).

[3] *Id.* at 2.

arm consumers and small businesses with the information they need to protect themselves from cyber threats. Given that the vast majority of cyber vulnerabilities stem from the lack of end user knowledge or awareness, an educational outreach program may be the most effective approach the Commission can take to help strengthen the overall security of the Internet.

II. An FCC Cybersecurity Roadmap Could Undermine and Unnecessarily Duplicate Ongoing Work.

A. The Proposed Roadmap Would Disclose Highly Sensitive Cybersecurity Information to Hostile Actors.

Sprint is concerned that the proposed Roadmap will divulge highly sensitive cybersecurity information to bad actors. Specifically, the PSHSB asks for "public input" on "a plan for the FCC to address vulnerabilities to core Internet protocols and technologies," which will "identify the five most critical cybersecurity threats to the communications infrastructure."[4] Cybersecurity vulnerability and threat information, however, is extremely sensitive, confidential data. Vulnerabilities are potential weaknesses or flaws that make a target more susceptible to exploitation and disruption. Detailed threat information may reveal the focus and attention of network service provider defensive measures at any given time.

Developing a Roadmap based on this sensitive information in the context of a public proceeding will expose these data to cyber criminals looking for any leads that may help them target their cyber assaults. If this information falls into the wrong hands, there is a real danger that hostile actors will direct their malicious activities against the specific vulnerabilities the Roadmap identifies, thus enhancing their ability to launch more effective cyber attacks. Accordingly, Sprint cautions that a Roadmap publicly disclosing sensitive, confidential

[4] *Id.* at 1.

communications network cybersecurity vulnerability and threat information will exacerbate cyber threats and could potentially affect national security.

B. The Proposed Roadmap Could Become Outdated and Hamper Network Service Provider Efforts to Combat Cyber Threats.

Sprint is also concerned that the proposed Roadmap not only may become outdated, but also may unintentionally impede network service provider efforts to counter cyber attacks. The proposed Roadmap will "establish a two-year plan, including milestones, for the FCC to address these threats."[5] A roadmap, which in this context is a plan that charts a course to move from point A to point B, typically envisions point B as a static end point. Cybersecurity, however, is a constant journey rather than a single trip with a final, set destination. As malicious actors worldwide continue to display remarkable technical ingenuity and tenacity in advancing their own cyber capabilities, cyber attacks continue to evolve and grow in speed and sophistication. For example, in 2009, more than 240 million distinct *new* malicious programs were identified, which represented a 100 percent increase over 2008.[6] Accordingly, in an environment where today's vulnerabilities and threats will not necessarily be tomorrow's, a two-year Roadmap will quickly be rendered obsolete.

Furthermore, a two-year Roadmap with fixed milestones could inadvertently hinder network service providers from exercising the maximum flexibility they need to tackle the challenges of the dynamic cyber threat landscape. As the vulnerabilities and threats evolve and

---

[5] *Id.*

[6] *Symantec Internet Security Threat Report, Cybercrime's Financial and Geographic Growth Shows No Slowdown during the Global Economic Crisis*, News Release, Symantec (April 20, 2010) *available at* http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf.

change, the tools and techniques carriers use to address them must evolve rapidly as well. As Commissioner Baker recognized, "ensur[ing] that network operators retain the flexibility and adaptability to respond to evolving cybersecurity threats" is critically important.[7] A two-year Roadmap requiring that fixed milestones be met, however, unintentionally could require providers to adopt technologies or practices that are outmoded or not appropriate for their unique circumstances. Consequently, a Roadmap may undermine their ability to mount the most effective cyber defense for their networks and customers.

C. Activities Addressing Communications Cybersecurity Vulnerability and Threat Issues are Ongoing.

Sprint notes that the work surrounding the proposed Roadmap may well duplicate efforts already underway at both the individual network service provider level and the communications sector level (within protected environments). Communications network service providers are constantly identifying and addressing cybersecurity vulnerabilities and threats on a daily basis to keep their networks fully operational. Enabling a customer's communications to flow seamlessly from one point to another is at the core of a communications network service provider's business. Cyber vulnerabilities and threats that interrupt or degrade those flows of communications can directly impair a provider's ability to provide its core service for its customers and thus can reduce its profitability. Therefore, every day providers develop, adopt and modify the tools, practices and technologies to identify vulnerabilities and "develop countermeasures and solutions in preparation for, and response to, cyber threats and attacks."[8]

---

[7] *Cyber Security Certification Program*, PS Docket No. 10-93, Notice of Inquiry, 25 FCC Rcd 4345 at Statement of Commissioner Meredith Attwell Baker (2010) (*Cyber Security Certification Program NOI*).

[8] *Public Notice* at 1.

In addition, the communications sector as a whole regularly plans for, identifies, and addresses cybersecurity vulnerabilities and threats through ongoing collaborative efforts within the Department of Homeland Security public-private partnership framework. For example, the Communications National Sector Risk Assessment ("NSRA"), conducted under this framework, identifies cyber vulnerabilities and threats to communications infrastructure across all segments of the communications sector, including broadcast, cable, satellite, wireless and wireline.[9] The 2008 NSRA, developed jointly by government representatives from the Communications Government Coordinating Council (CGCC) and industry representatives from the Communications Sector Coordinating Council (CSCC), was conducted with the appropriate information protections and remains a confidential document. The CGCC and CSCC are dedicating resources to work on the next NSRA, which is currently in progress.

Accordingly, it appears that the proposed Roadmap would duplicate ongoing work specifically aimed at identifying and addressing communications cybersecurity vulnerabilities and threats. As Commissioner Baker cautioned, any decisions should be "made in close coordination with other governmental efforts, particularly those of the Department of Homeland Security," and that the Commission "should ensure our actions do not add additional layers of requirements or duplicative obligations on providers."[10] Otherwise, the resources diverted to

---

[9] The communications sector conducted the NSRA pursuant to the Communications Sector Specific Plan ("CSSP") under the construct of the National Infrastructure Protection Plan ("NIPP"). The CSSP provides additional information regarding the NSRA purpose and process. *See Communications Critical Infrastructure and Key Resources Sector-Specific Plan as an Input to the National Infrastructure Protection Plan*, Department of Homeland Security (May 2007) *available at* http://www.dhs.gov/xlibrary/assets/nipp-ssp-communications.pdf.

[10] *Cyber Security Certification Program NOI* at Statement of Commissioner Meredith Attwell Baker.

comply with multiple, duplicative requirements would no longer be available to invest in cyber counter measures and develop new approaches to combat cyber threats.

III. The Commission's Role within the Emerging Cybersecurity Framework is Undefined.

As part of its inquiry, the PSHSB asks what role, if any, the Commission should play in addressing cyber vulnerabilities and how the Commission should coordinate its efforts with other government agencies.[11] Sprint submits that the Commission's role within the emerging federal cybersecurity framework has not yet been defined. Several ongoing federal initiatives, which aim to coordinate and improve the overall cyberspace posture of the United States, could affect the Commission's activity in this area. For example, one of the near-term action items identified in the White House *Cyberspace Policy Review* is to update and advance implementation of the national strategy to secure information and communications infrastructure.[12] That updated strategy may shed light upon the Commission's role in the cybersecurity arena, including whether it is the appropriate entity to address cybersecurity vulnerabilities and threats.

In addition, federal legislation is well underway to develop a centralized, comprehensive approach to cybersecurity, which covers not only the communications sector, but the entire cyber ecosystem. Under such legislation, authority and responsibility for cybersecurity matters, including vulnerability and threat issues, may fall to another federal department or agency. For example, the proposed *Protecting Cyberspace as a National Asset Act of 2010* gives the

---

[11] *Public Notice* at 2.

[12] *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* at 37 (White House, 2009) (*Cyberspace Policy Review*). *See also Cybersecurity Progress after President Obama's Address*, National Security Council (July 14, 2010), *available at* http://www.whitehouse.gov/administration/eop/nsc/cybersecurity/progressreports/july2010.

Department of Homeland Security central responsibility for federal cybersecurity matters.[13] If the Commission proceeds with the Roadmap or similar cybersecurity activities for which another government entity is responsible, it runs the risk of implementing duplicative or conflicting requirements, which would counter its end goal of enhancing cybersecurity.

In the meantime, whether and to what extent the Commission has a cybersecurity role under current law has not yet been determined. As the Commission itself appears to recognize, it may not, in light of the D.C. Circuit's recent decision in *Comcast Corp. v. FCC*,[14] have the authority under the Communications Act to regulate the provision of IP-based broadband service and the facilities over which such services are provided.[15] To address this uncertainty, the Commission's pending Notice of Inquiry is examining possible legal frameworks for broadband Internet access services.[16] The ultimate outcome of the *Broadband NOI*, however, may not give the Commission the requisite jurisdiction to establish a Roadmap or otherwise engage in related cybersecurity activities. Accordingly, in light of pending federal initiatives as well as the *Broadband NOI*, Sprint suggests that the Commission suspend consideration of the Roadmap and related cybersecurity activities until its role and authority within the new federal cybersecurity landscape is defined.

---

[13] *See Protecting Cyberspace as a National Asset Act of 2010,* S. 3480, 111th Cong. (2010).

[14] *Comcast Corp. v. FCC*, 600 F.3d 642 (D.C. Cir. 2010).

[15] *Cyber Security Certification Program NOI* at ¶¶10-11.

[16] *Framework for Broadband Internet Service,* Notice of Inquiry, GN Docket No. 10-127, 25 FCC Rcd 7866 at ¶ 2 (2010) (*Broadband NOI*).

IV. The Commission Can Take Other Important Steps to Advance Cybersecurity.

Sprint believes that the Commission can take two important, concrete steps to advance its general cybersecurity goals. *First,* Sprint suggests that the Commission continue to support and promote CSRIC's cybersecurity best practices work under its current chartered term and into the future. CSRIC is charged with providing "recommendations to the FCC to ensure optimal security, reliability and interoperability of communications systems, including telecommunications, media and public safety communications."[17] As part of its chartered responsibilities, CSRIC established Working Group 2A to review and update the more than 200 cybersecurity best practices that the Network Reliability and Interoperability Council ("NRIC") originally developed for the communications sector to meet today's cyber challenges.[18]

The NRIC/CSRIC best practices are critical to the industry because they provide communications service providers, both large and small, expert recommendations on cybersecurity practices that may be effective and feasible. Such recommendations include those that help address communications infrastructure vulnerabilities and threats. In addition, the NRIC/CSRIC best practices approach offers providers the flexibility to adopt them in whole or in part as appropriate for their particular networks, systems, and processes.[19] Furthermore, with the

---

[17] Charter of the FCC's Communications Security, Reliability, and Interoperability Council 1, *available at* http://www.fcc.gov/pshs/docs/advisory/csric/CSRC_charter_03-19-2009.pdf.

[18] *See CSRIC Working Group Descriptions*, *available at* http://www.fcc.gov/pshs/advisory/csric/wg-descriptions.pdf. Working Group 2A -- Cyber Security Best Practices will review cyber security best practices based on previous work under NRIC VI and VII.

[19] As Focus Group 2B (Homeland Security – Cyber Security) of NRIC VII recognized, "[n]ot all Best Practices will apply to all companies nor are there Best Practices for all situations in which a company may find a cyber security problem." *Summary of Activities, Guidance and*

CSRIC framework already in place, voluntary best practices can be updated quickly, which is important given that cybersecurity is a moving target requiring continual refinement. Therefore, it is important that the Commission continue to support regular updates of CSRIC cybersecurity best practices going forward to help providers keep pace with rapid advances in state of the art cybersecurity measures.

Second, Sprint proposes that the Commission explore the possibility of promoting consumer cybersecurity education and awareness in conjunction with other federal agencies. Given the interdependent nature of the Internet, cybersecurity is only as strong as its weakest link. End users are considered the most vulnerable link, and that vulnerability typically stems from lack of knowledge or awareness.[20] End users need information on how to protect themselves from cyber threats, such as web-based malware, social engineering schemes, and virus attacks.[21]

Backed by its experience in communicating technical advice to the public in a clear, understandable way using multiple forms of media, the Commission is well positioned to either launch its own campaign or lend its expertise to other federal cybersecurity public awareness campaigns targeting consumers and small businesses.[22] The Commission's DTV transition

---

Cybersecurity Issues, Focus Group 2B, *available at* http://www.nric.org/meetings/docs/meeting_20051216/FG2B_Dec%2005_Final%20Report.pdf.

[20] *See State of the Web – Q4 2009, A View of the Web from an End User's Perspective*, Zsacaler Labs at 19, *available at* http://www.zscaler.com/pdf/industryreports/state_of_the_web_q4_2009_noapp.pdf.

[21] As the President's *Cyberspace Policy Review* notes, "[p]eople cannot value security without first understanding how much is at risk." *Cyberspace Policy Review* at iv.

[22] For example, the Department of Homeland Security is a sponsor of National Cybersecurity Awareness Month in October 2010 to help focus public attention on reducing vulnerability and

education campaign is an excellent example of a comprehensive campaign to help guide consumers through a thicket of advanced technical information and provide them direction. More recently, the Commission's *Wireless World Travel Week* offered travelers important money-saving tips on international wireless service, using the Commission's "Savvy Traveler" blog posts and Twitter page, a video, and a tip sheet for consumers.[23]

In a cybersecurity awareness campaign, the Commission, using multiple forms of media, could help educate end users about the various types of threats, how to protect themselves from such threats (*e.g.,* password management, installing and maintaining anti-virus software and firewalls, using caution with e-mail attachments, avoiding phishing scams), and the steps to take if they become victims of a cyber intrusion. Combining the expertise of both the PSHSB and the Consumer and Government Affairs Bureau should help produce or contribute to an effective outreach program to help arm consumers and small businesses with the knowledge they need to combat cyber threats.

V. Conclusion

For the foregoing reasons, Sprint respectfully suggests that the Commission refrain from developing the proposed Cybersecurity Roadmap. Instead, the Commission should continue to support CSRIC best practices work and explore launching or lending its expertise toward a cybersecurity education and awareness program for consumers and small businesses to help advance its policy objectives.

---

improving resilience to cyber attacks. (*See* http://staysafeonline.mediaroom.com/index.php?s=43&item=61.)

[23] *FCC Announces Wireless World Travel Week; FCC and Wireless Providers Offer Money-Saving Calling Tips for Foreign Travel*, News Release, rel. June 21, 2010.

Respectfully submitted,

SPRINT NEXTEL CORPORATION

/s/ Charles W. McKee
Charles W. McKee
Vice President, Government Affairs
Federal & State Regulatory

Maria L. Cattafesta
Senior Counsel, Government Affairs

Sprint Nextel Corporation
900 7th Street, N.W., Suite 700
Washington, D.C. 20001
703-433-3786

September 23, 2010